(Translation of the front page
of the priority document of
Japanese Patent Application
No. 2001-190445)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application : May 22, 2001

Application Number : Patent Application
2001-190445

Applicant(s) : Humming Heads Inc.

November 9, 2001

Commissioner,
Japan Patent Office Kouzo Oikawa

Certification Number 2001-3098289

OIPE JC139
JAN 16 2002
PATENT & TRADEMARK OFFICE

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

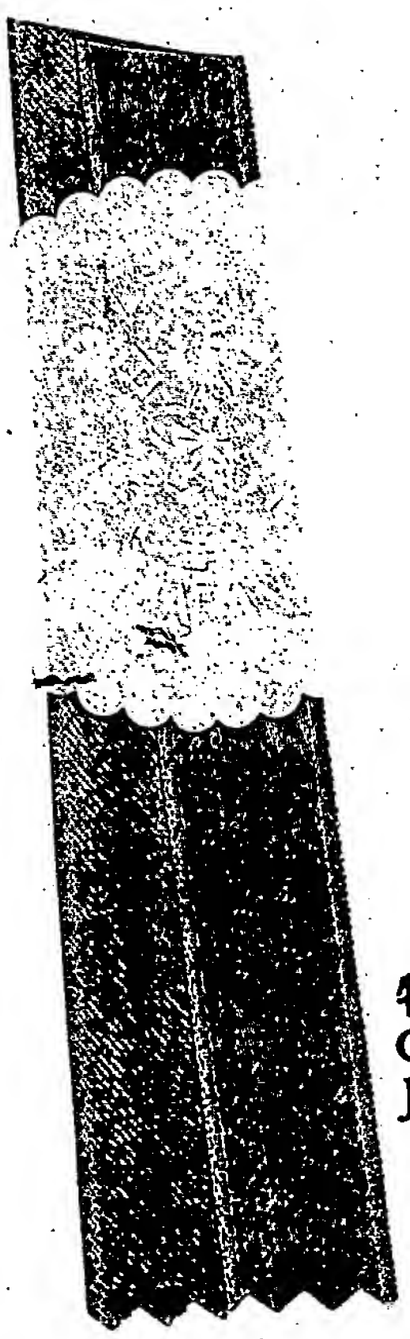
This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　５月２２日

出願番号
Application Number: 特願２００１－１９０４４５

出願人
Applicant(s): ハミングヘッズ株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT



２００１年１１月　９日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０９８２８９

【書類名】　特許願

【整理番号】　HH08PH1302

【提出日】　平成13年 5月22日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/00

【発明者】

【住所又は居所】　東京都中央区月島一丁目２番１３号　ハミングヘッズ株式会社内

【氏名】　大江　尚之

【発明者】

【住所又は居所】　東京都中央区月島一丁目２番１３号　ハミングヘッズ株式会社内

【氏名】　志摩　貴浩

【特許出願人】

【識別番号】　500083226

【住所又は居所】　東京都中央区月島一丁目２番１３号

【氏名又は名称】　ハミングヘッズ株式会社

【代表者】　大江　尚之

【電話番号】　03-3531-7281

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【書類名】　　明細書

【発明の名称】　電子情報に対する操作を制御する情報処理装置及びその方法、情報処理システム、プログラム

【特許請求の範囲】

【請求項１】　電子情報を変換して操作を制限する情報処理装置であって、

電子情報を読み込み記憶する第１の記憶手段と、

電子情報に対する操作を制限する内容を定義した制限属性情報を、前記第１の手段で記憶した電子情報に付加する第２の手段と、

電子情報に対する操作を監視し制御する制限プログラムを前記第１の手段で記憶した電子情報に付加する第３の手段と、

前記第１の手段で記憶した電子情報に前記第２の手段及び前記第３の手段によって付加したデータをまとめて実行可能な形式で出力する第４の手段と

を備えることを特徴とする情報処理装置。

【請求項２】　前記第４の手段にて出力された実行可能形式データを利用する情報処理装置であって、

実行可能形式データを起動する第５の手段と、

前記第３の手段で付加した制限プログラムから電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する第６の手段と、

前記第２の手段で付加された制限属性情報から対象アプリケーションを取得する第７の手段と、

前記第７の手段で取得したアプリケーションを起動する第８の手段と、

前記第８の手段が成功したかどうかを判定する第９の判定手段と、

前記第９の判定結果でアプリケーションの起動が失敗した場合は、前記第５の手段で実行した実行可能形式データを終了する第１０の手段と、

前記第９の判定結果でアプリケーションの起動が成功した場合は、元の電子情報を復元しアプリケーションからの操作が可能な状態にする第１１の手段と、

前記第１１の手段で復元した電子情報を前記第８で起動したアプリケーションに渡す第１２の手段と

を備えることを特徴とする情報処理装置。

【請求項３】　前記第２の手段において制限属性情報にアプリケーション情報を含まず、前記第７の手段に代わって前記第８の手段で起動すべきアプリケーションを自動認識する第１３の手段

を備えることを特徴とする情報処理装置。

【請求項４】　前記８の手段で起動したアプリケーションが前記１２の手段で渡した電子情報を解放した場合に、前記第１１の手段で復元した電子情報を受け取り側情報処理装置から抹消する第１４の手段と、

前記８の手段で起動したアプリケーションが終了した場合に、前記第６の手段で起動した制限ルーチンを終了し、受け取り側情報処理装置から抹消する第１５の手段と

を備えることを特徴とする情報処理装置。

【請求項５】　電子情報を変換して操作を制限する情報処理方法であって、

電子情報を読み込み記憶する第１の工程と、

電子情報に対する操作を制限する内容を定義した制限属性情報を、前記第１の工程で記憶した電子情報に付加する第2の工程と、

電子情報に対する操作を監視し制御する制限プログラムを前記第１の工程で記憶した電子情報に付加する第３の工程と、

前記第１の工程で記憶した電子情報に前記第２の工程及び前記第３の工程によって付加したデータをまとめて実行可能な形式で出力する第４の工程と

を備えることを特徴とする情報処理方法。

【請求項６】　前記第４の工程にて出力された実行可能形式データを利用する情報処理方法であって、

実行可能形式データを起動する第５の工程と、

前記第３の工程で付加した制限プログラムから電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する第６の工程と、

前記第２の工程で付加された制限属性情報から対象アプリケーションを取得する第７の工程と、

前記第７の工程で取得したアプリケーションを起動する第８の工程と、

前記第８の工程が成功したかどうかを判定する第９の判定工程と、

前記第９の判定結果でアプリケーションの起動が失敗した場合は、前記第５の工程で実行した実行可能形式データを終了する第１０の工程と、

前記第９の判定結果でアプリケーションの起動が成功した場合は、元の電子情報を復元しアプリケーションからの操作が可能な状態にする第１１の工程と、

前記第１１の工程で復元した電子情報を前記第８で起動したアプリケーションに渡す第１２の工程と

を備えることを特徴とする情報処理方法。

【請求項７】　前記第２の工程において制限属性情報にアプリケーション情報を含まず、前記第７の工程に代わって前記第８の工程で起動すべきアプリケーションを自動認識する第１３の工程

を備えることを特徴とする情報処理方法。

【請求項８】　前記８の工程で起動したアプリケーションが前記１２の工程で渡した電子情報を解放した場合に、前記第１１の工程で復元した電子情報を受け取り側情報処理装置から抹消する第１４の工程と、

前記８の工程で起動したアプリケーションが終了した場合に、前記第６の工程で起動した制限ルーチンを終了し、受け取り側情報処理装置から抹消する第１５の工程と

を備えることを特徴とする情報処理方法。

【請求項９】　複数の端末群が通信網を介して相互に接続されて構成される情報処理システムであって、

前記複数の端末群それぞれは、

電子情報提供側の端末は、前記請求項１の情報処理装置を備え、

電子情報受け取り側端末は、前記請求項２または前記請求項３または前記請求項４の情報処理装置を備え、

電子情報提供側の端末から前記請求項１の情報処理装置によって出力された実行可能な形式の情報を、電子情報受け取り側の端末に送信する送信手段と、

前記電子情報提供側端末から送信された実行可能な形式の情報を、電子情報受け取り側の端末にて受信する受信手段と

を備えることを特徴とする情報処理装置システム。

【請求項１０】　電子情報を変換して操作を制限する情報処理をコンピュータに機能させるプログラムであって、

電子情報を読み込み記憶する第１の記憶プログラムコードと、

電子情報に対する操作を制限する内容を定義した制限属性情報を、前記第１のプログラムコードで記憶した電子情報に付加する第２のプログラムコードと、

電子情報に対する操作を監視し制御する制限プログラムを前記第１のプログラムコードで記憶した電子情報に付加する第３のプログラムコードと、

前記第１のプログラムコードで記憶した電子情報に前記第２のプログラムコード及び前記第３のプログラムコードによって付加したデータをまとめて実行可能な形式で出力する第４のプログラムコードと

を備えることを特徴とするプログラム。

【請求項１１】　前記第４のプログラムコードにて出力された実行可能形式データを利用する情報処理をコンピュータに昨日させるプログラムであって、

実行可能形式データを起動する第５のプログラムコードと、

前記第３のプログラムコードで付加した制限プログラムから電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する第６のプログラムコードと、

前記第２のプログラムコードで付加された制限属性情報から対象アプリケーションを取得する第７のプログラムコードと、

前記第７のプログラムコードで取得したアプリケーションを起動する第８のプログラムコードと、

前記第８のプログラムコードが成功したかどうかを判定する第９の判定プログラムコードと、

前記第９の判定結果でアプリケーションの起動が失敗した場合は、前記第５のプログラムコードで実行した実行可能形式データを終了する第１０のプログラムコードと、

前記第９の判定結果でアプリケーションの起動が成功した場合は、元の電子情報を復元しアプリケーションからの操作が可能な状態にする第１１のプログラムコードと、

前記第１１のプログラムコードで復元した電子情報を前記第８で起動したアプリケーションに渡す第１２のプログラムコードと

を備えることを特徴とするプログラム。

【請求項１２】　前記第２のプログラムコードにおいて制限属性情報にアプリケーション情報を含まず、前記第７のプログラムコードに代わって前記第８のプログラムコードで起動すべきアプリケーションを自動認識する第１３のプログラムコード

を備えることを特徴とするプログラム。

【請求項１３】　前記８のプログラムコードで起動したアプリケーションが前記１２のプログラムコードで渡した電子情報を解放した場合に、前記第１１のプログラムコードで復元した電子情報を受け取り側情報処理装置から抹消する第１４のプログラムコードと、

前記８のプログラムコードで起動したアプリケーションが終了した場合に、前記第６のプログラムコードで起動した制限ルーチンを終了し、受け取り側情報処理装置から抹消する第１５のプログラムコードと

を備えることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ファイル、電子メール、Ｗｅｂ情報等のコンピュータで利用する電子情報に対する操作を制御する情報処理装置及びその方法、情報処理システム及びそれらの制御方法、プログラムに関するものである。

【０００２】

【従来の技術】

コンピュータ、携帯端末、インターネット等の普及に伴い、電子情報が一般的に利用されるようになり、特に、電子情報の共有利用や、電子情報による情報の受け渡しが、一般的なアプリケーションを用いて容易に行える環境になっている。

ところが、一般的なアプリケーションを用いて容易に電子情報が利用できるが

ゆえに、アプリケーションが実装する機能の範囲で電子情報を自由に利用でき、電子情報に対する特定の操作を制限する為には、アプリケーションの機能に依存するか、オペレーションシステム（以下、ＯＳ）のアクセス制御機能を用いて利用自体を禁止するか、もしくは利用する環境にあらかじめ制限したい操作を制御するプログラム等を導入しておく必要があった。

【０００３】

【発明が解決しようとする課題】

電子情報に対する操作を上記の従来方法で制限する場合、電子情報ごとに柔軟な制限を実現することは不可能である。例えば、印刷操作を禁止したい電子情報がある場合、アプリケーションの機能に依存する方法では、そのアプリケーションが印刷禁止機能を実装していなければ実現できない。また、ＯＳのアクセス制御機能を利用する場合も、一般的なＯＳ（例えば、Ｗｉｎｄｏｗｓ、ＵＮＩＸ等）においては、印刷を制限する機能は実装されていないため、参照そのものを禁止する方法を採ることになる。さらに、あらかじめ特別なプログラムを導入する場合には、そのプログラムが導入されていない環境では制限できない、もしくはそのプログラムが実装していない制限事項については実現できない。

【０００４】

上記の例のように、電子情報ごとに特定の操作を制限したい場合、実現できないか、必要以上に制限をかけるため電子情報が十分利用できなくなるなどの問題があった。

【０００５】

本発明は、上記の課題を解決するためになされたものであり、電子情報における共有利用の促進と、電子情報ごとに必要な制限すべき操作の禁止を、効率的に実現することができる情報処理装置及びその方法、情報処理システム及びそれらの制御方法、プログラムを提供することを目的とする。

【０００６】

【課題を解決するための手段】

上記目的を達成するための本発明による情報処理装置は以下の構成を備える。すなわち、

電子情報提供側の情報処理装置においては、電子情報に対する操作を制限するよう電子情報をプロテクション化する情報処理装置であって、

対象の電子情報にアクセス可能なコンピュータと、対象の電子情報およびプロテクション化電子情報を格納するメモリもしくはハードディスクなどの記憶媒体と、電子情報を提供するための手段としてフロッピーディスクドライブなどの外部メディア装置もしくは通信回線等を備える。

一方、電子情報受け取り側の情報処理装置においては、プロテクション化電子情報を利用する情報処理装置であって、

受け取ったプロテクション化電子情報にアクセス可能であり対象の電子情報が利用可能なコンピュータと、プロテクション化電子情報および対象の電子情報を一時的に格納するメモリもしくはハードディスクなどの記憶媒体と、電子情報の利用内容に応じてディスプレイ、プリンタ、キーボード等の入出力装置と、プロテクション化電子情報を受け取るための手段としてフロッピーディスクドライブなどの外部メディア装置もしくは通信回線等を備える。

【０００７】

ここで、プロテクション化電子情報とは、対象の電子情報に対する操作を制御する制限プログラムと、電子情報に対して印刷禁止や複製禁止といった制限する操作の内容を定義した制限属性を、対象の電子情報に付加し、実行可能形式にしたものである。

対象の電子情報に対して制限プログラムと制限属性を付加することで元の電子情報を変換する処理をプロテクション化と呼び、プロテクション化した電子情報をプロテクション化電子情報と呼ぶことにする。また、プロテクション化を実現するプログラムをプロテクション化プログラムと呼ぶことにする。

【０００８】

また、制限プログラムは、プロテクション化電子情報を元の電子情報として利用可能にするための展開ルーチン部と、電子情報へのアクセスを制御するための制限ルーチン部からなる。

【０００９】

さらに、制限属性は、電子情報に対して制限する操作と条件の組を１組以上保

持し、必要に応じて、電子情報にアクセスするためのアプリケーション等のプログラムを特定する情報を保持する。

【００１０】

ここで、アプリケーションとは、電子情報にアクセスするために使用されるプログラムを指し、例えば、文書ファイルにアクセスするためのワープロソフトや、画像や動画を再生または編集するプログラムなどがそれに相当する。

アプリケーションはユーザが必ずしも操作するものとは限らず、一般的にＯＳもしくはプラットフォームの機能を利用して電子情報にアクセスするプログラムを、総称してここではアプリケーションと呼ぶことにする。

【００１１】

また、ＯＳ（オペレーティングシステム）にはマイクロソフト社のＷｉｎｄｏｗｓやアップル社のＭａｃＯＳ、さらに一般的にＵＮＩＸと呼ばれるものがあり、携帯端末機などでもＯＳは稼動している。さらに、ここでいうプラットフォームとは、ＯＳのことを指すこともあるが、より広く、Ｗｅｂ情報を閲覧するブラウザソフトなども、電子情報を扱う汎用的な環境を提供し、その上で実行可能な形式のプログラムを実行することができるコンピュータ上の基本プログラムという意味で、プラットフォームに含めることにする。

【００１２】

本発明の電子情報を提供する側の情報処理装置にはプロテクション化プログラムが組み込まれており、プロテクション化プログラムは、対象となる電子情報を読み込む第１の手段と、電子情報に対して制限する操作の情報と電子情報を利用するためのアプリケーション等の情報が定義された制限属性情報を前記第１の手段で読み込んだ電子情報に付加する第２の手段と、電子情報に対する操作を監視し制御する制限プログラムを前記第１の手段で読み込んだ電子情報に付加する第３の手段と、前記第１の手段で読み込んだ電子情報に前記第２の手段及び前記第３の手段によって付加したデータをまとめてプロテクション化電子情報として実行可能な形式で出力する第４の手段とを備える。

【００１３】

また、本発明の電子情報を受け取る側の情報処理装置ではプロテクション化電

子情報の実行が可能であり、プロテクション化電子情報を実行した際の処理は、プロテクション化電子情報を起動する第５の手段と、前記第３の手段で付加した制限プログラムから電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する第６の手段と、前記第２の手段で付加された制限属性情報から対象アプリケーションを取得する第７の手段と、前記第７の手段で取得したアプリケーションを起動する第８の手段と、前記第８の手段が成功したかどうかを判定する第９の手段と、前記第９の判定結果でアプリケーションの起動が失敗した場合はプロテクション化電子情報の実行を終了する第１０の手段と、前記第９の判定結果でアプリケーションの起動が成功した場合は元の電子情報を復元しアプリケーションからの操作が可能な状態する第１１の手段と、前記第１１の手段で復元した電子情報を前記第８の手段によって起動したアプリケーションに渡す第１２の手段とを備える。

【００１４】

また、前記第２の手段において制限属性情報にアプリケーション情報を含まず前記第７の手段の代わりに前記第８の手段で起動すべきアプリケーションを自動認識する第１３の手段を備える。

前記第１３の手段における自動認識の例としては、電子情報がファイルである場合にはその拡張子からアプリケーションがＯＳによって定義されている場合がある。また、電子情報を受け取る側の環境によってはアプリケーションが特定できる場合がある。このように電子情報を利用する際に使用するアプリケーションが自明である場合には、前記第２の手段における制限属性内にアプリケーション情報は必要ではなく、前記第１３の手段において起動すべきアプリケーションの自動認識が可能となる。

【００１５】

また、前記８の手段で起動したアプリケーションが前記１２の手段で渡した電子情報を解放した場合に前記第１１の手段で復元した電子情報を受け取り側情報処理装置から抹消する第１４の手段と、前記８の手段で起動したアプリケーションが終了した場合に前記第６の手段で起動した制限ルーチンを終了し受け取り側情報処理装置から抹消する第１５の手段とを備える。

【００１６】

上記目的を達成するための本発明による情報処理方法は以下の構成を備える。すなわち、

電子情報を提供する側においては、電子情報をプロテクション化する情報処理方法であって、

対象となる電子情報を読み込み記憶する第１の工程と、電子情報に対して制限する操作の情報と電子情報を利用するためのアプリケーション等の情報が定義された制限属性情報を前記第１の工程で読み込んだ電子情報に付加する第２の工程と、電子情報に対する操作を監視し制御する制限プログラムを前記第１の工程で読み込んだ電子情報に付加する第３の工程と、前記第１の工程で読み込んだ電子情報に前記第２の工程及び前記第３の工程によって付加したデータをまとめてプロテクション化電子情報として実行可能な形式で出力する第４の工程とを備える。

【００１７】

また、電子情報を受け取る側においては、プロテクション化電子情報を利用するための情報処理方法であって、

実行可能な形式であるプロテクション化電子情報を起動する第５の工程と、前記第３の工程で付加した制限プログラムから電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する第６の工程と、前記第２の工程で付加された制限属性情報から対象アプリケーションを取得する第７の工程と、前記第７の工程で取得したアプリケーションを起動する第８の工程と、前記第８の工程が成功したかどうかを判定する第９の判定工程と、前記第９の判定結果でアプリケーションの起動が失敗した場合はプロテクション化電子情報の実行を終了する第１０の工程と、前記第９の判定結果でアプリケーションの起動が成功した場合は元の電子情報を復元しアプリケーションからの操作が可能な状態にする第１１の工程と、前記第１１の工程で復元した電子情報を前記第８の工程によって起動したアプリケーションに渡す第１２の工程とを備える。

【００１８】

また、前記第２の工程において制限属性情報にアプリケーション情報を含まず

前記第７の工程の代わりに前記第８で起動すべきアプリケーションを自動認識する第１３の手段を特徴とする。

前記第１３の工程における自動認識の例としては、電子情報がファイルである場合にはその拡張子からアプリケーションがＯＳによって定義されている場合がある。また、電子情報を受け取る側の環境によってはアプリケーションが特定できる場合がある。このように電子情報を利用する際に使用するアプリケーションが自明である場合には、前記第２の工程における制限属性内にアプリケーション情報は必要ではなく、前記第１３の工程において起動すべきアプリケーションの自動認識が可能となる。

【００１９】

また、前記８の工程で起動したアプリケーションが前記１２の工程で渡した電子情報を解放した場合に前記第１１の工程で復元した電子情報を受け取り側情報処理装置から抹消する第１４の工程と、前記８の工程で起動したアプリケーションが終了した場合に前記第６の工程で起動した制限ルーチンを終了し受け取り側情報処理装置から抹消する第１５の工程とを備える。

【００２０】

上記目的を達成するための本発明による情報処理システムは以下の構成を備える。すなわち、

複数の端末群が通信網を介して相互に接続されて構成される情報処理システムであって、

前記複数の端末群それぞれにおいて、

電子情報提供側の端末は、前記第１の手段、前記第２の手段、前記第３の手段および前記第４の手段を備えた情報処理装置であって、

電子情報受け取り側端末は、前記第５の手段、前記第６の手段、前記第７の手段、前記第８の手段、前記第９の手段、前記第１０の手段、前記第１１の手段および前記第１２の手段、または前記第１２の手段、または前記第１３の手段および前記第１４の手段を備えた情報処理装置であって、

前記電子情報提供側の情報処理装置によって出力された実行可能な形式の情報を、前記電子情報受け取り側の情報処理装置に送信する送信手段と、

前記電子情報提供側の情報処理装置から送信された実行可能な形式の情報を、前記電子情報受け取り側の情報処理装置にて受信する受信手段と

を備える。

【００２１】

上記目的を達成するための本発明によるプログラムは以下の構成を備える。すなわち、

電子情報提供側においては、電子情報に対する操作を制限するよう電子情報をプロテクション化するプログラムであって、

対象となる電子情報を読み込み記憶する第１のプログラムコードと、電子情報に対して制限する操作の情報と電子情報を利用するためのアプリケーション等の情報が定義された制限属性情報を前記第１のプログラムコードで読み込んだ電子情報に付加する第２のプログラムコードと、電子情報に対する操作を監視し制御する制限プログラムを前記第１のプログラムコードで読み込んだ電子情報に付加する第３のプログラムコードと、前記第１のプログラムコードで読み込んだ電子情報に前記第２のプログラムコード及び前記第３のプログラムコードによって付加したデータをまとめてプロテクション化電子情報として実行可能な形式で出力する第４のプログラムコードとを備える。

【００２２】

また、電子情報を受け取る側においては、プロテクション化電子情報を利用するためのプログラムであって、

実行可能な形式であるプロテクション化電子情報を起動する第５のプログラムコードと、前記第３のプログラムコードで付加した制限プログラムから電子情報に対する操作を監視及び制御する制限ルーチン部を読み込み起動する第６のプログラムコードと、前記第２のプログラムコードで付加された制限属性情報から対象アプリケーションを取得する第７のプログラムコードと、前記第７のプログラムコードで取得したアプリケーションを起動する第８のプログラムコードと、前記第８のプログラムコードが成功したかどうかを判定する第９の判定プログラムコードと、前記第９の判定結果でアプリケーションの起動が失敗した場合はプロテクション化電子情報の実行を終了する第１０のプログラムコードと、前記第９

の判定結果でアプリケーションの起動が成功した場合は元の電子情報を復元しアプリケーションからの操作が可能な状態する第１１のプログラムコードと、前記第１１のプログラムコードで復元した電子情報を前記第８のプログラムコードで起動したアプリケーションに渡す第１２のプログラムコードとを備える。

【００２３】

また、前記第２のプログラムコードにおいて制限属性情報にアプリケーション情報を含まず前記第７のプログラムコードの代わりに前記第８のプログラムコードで起動すべきアプリケーションを自動認識する第１３のプログラムコードを備える。

前記第１３のプログラムコードにおける自動認識の例としては、電子情報がファイルである場合にはその拡張子からアプリケーションがＯＳによって定義されている場合がある。また、電子情報を受け取る側の環境によってはアプリケーションが特定できる場合がある。このように電子情報を利用する際に使用するアプリケーションが自明である場合には、前記第２のプログラムコードにおける制限属性内にアプリケーション情報は必要ではなく、前記第１３のプログラムコードにおいて起動すべきアプリケーションの自動認識が可能となる。

【００２４】

また、前記８のプログラムコードで起動したアプリケーションが前記１２のプログラムコードで渡した電子情報を解放した場合に前記第１１のプログラムコードで復元した電子情報を受け取り側情報処理装置から抹消する第１４のプログラムコードと、前記８のプログラムコードで起動したアプリケーションが終了した場合に前記第６のプログラムコードで起動した制限ルーチンを終了し受け取り側情報処理装置から抹消する第１５のプログラムコードとを備える。

【００２５】

なお、前記制限プログラムの内容は、アプリケーションが電子情報にアクセスする際にその要求を捕捉し、制限情報にしたがってアクセスの可否を判定し、判定の結果によってはアクセスを拒否するというものであり、詳細については特願２０００－３５２１１３にて開示してある。

【００２６】

発明者は本装置をＨ．Ｈ電子情報プロテクション化方式と命名した。

【００２７】

【発明の実施の形態】

以下、本発明の実施の形態を図面により詳細に説明する。

【００２８】

【第１の実施形態】

図１は本発明を実施する環境の第１の実施形態を示すハードウェア構成図である。

図１に示す構成は、プロテクション化電子情報を提供する情報処理装置１０と電子情報を受け取り利用するための情報処理装置１１とプロテクション化電子情報を受け取り側へ送信することが可能な通信回線１２からなるハードウェア構成を示すものである。

【００２９】

提供側の情報処理装置１０は、ハードディスク（ＨＤＤ）１０３を備えたコンピュータ（ＰＣ）１００、外部にプロテクション化電子情報を出力することが可能な外部装置（ＦＤＤ）１０２で構成され、対象の電子情報１０１を保持している。

一方、受け取り側の情報処理装置１１は、ハードディスク（ＨＤＤ）１１２を備えたコンピュータ（ＰＣ）１１０、外部からプロテクション化電子情報を読み込むことが可能な外部装置（ＦＤＤ）１１３、ディスプレイ１１６、プリンタ１１５、キーボード１１４で構成され、受け取ったプロテクション化電子情報１１１を保持している。

提供側の情報処理装置１０と受け取り側の情報処理装置１１は、通信網１２を利用して電子情報の受け渡しが可能となっている。

【００３０】

コンピュータ１００には、汎用のＯＳまたはプラットフォームが組み込まれており、さらに本発明に係るプロテクション化プログラムが組み込まれている。

コンピュータ１１０には、汎用のＯＳと受け取った電子情報にアクセスするためのアプリケーションが組み込まれている。

【００３１】

提供側では、提供する電子情報１０１をプロテクション化プログラムによってプロテクション化し、プロテクション化電子情報を作成する。作成したプロテクション化電子情報を外部装置１０２もしくは通信網１２を介して受け取り側に渡し、受け取り側の情報処理装置では、外部装置１１３もしくは通信網１２を介してプロテクション化電子情報を受け取る。受け取ったプロテクション化電子情報を実行することで、目的の電子情報を利用可能となるが、プロテクション化によって利用範囲は制限される。例えば、印刷操作の禁止や利用ユーザの限定などである。

このように、本発明では、受け取り側に制限操作を定義したプロテクション化電子情報を渡すことによって、提供側は利用範囲を限定した形で電子情報を提供することが可能となる。

【００３２】

図２（ａ）は、本発明に係るプロテクション化電子情報の構成を示す図であり、プロテクション化電子情報２０は制限プログラム２１、制限属性２２、制限対象の元電子情報２３から構成されており、さらに図２（ｂ）に示すように制限プログラム２１は展開ルーチン部２１０と制限ルーチン部２１１から構成され、また図２（ｃ）に示すように制限属性２２は対象アプリケーション情報２２０、制限操作情報２２１１、制限条件情報２２２１から構成される。制限操作情報と制限条件情報の組は必要に応じて複数保持することがあり、それぞれ制限操作情報２２１Ｎ、制限条件情報２２２Ｎまで保持している状態を示している。

【００３３】

制限操作情報としては、アプリケーション、ＯＳまたはプラットフォームに実装されている機能のうち、制限したい機能を指定する。例えば、印刷、編集、表示、画面のハードコピー、外部装置への保存などである。

制限条件としては、操作を制限するための条件を指定する。例えば、利用可能な時間の指定、利用可能なコンピュータの指定、利用可能なユーザやグループの指定、課金条件などである。

無条件に特定の操作を制限する場合は、制限条件を省略する。

【００３４】

また、対象アプリケーションが自明であるような場合には、対象アプリケーション情報２２０は省略されることもある。例えば、Ｗｉｎｄｏｗｓでは対象ファイルの拡張子によってアプリケーションが特定されることがあり、これは対象アプリケーションが自明なケースである。

逆に、対象アプリケーションを明示することで、電子情報にアクセスするアプリケーションを限定することが可能となる。

【００３５】

制限ルーチン部２１１は、対象の電子情報に対する操作を監視及び制御するプログラムコードが実装されており、その内容および実現方法については特願２０００－３５２１１３にて開示してある。

【００３６】

図３は、本発明におけるプロテクション化の手順を示すフロー図である。

【００３７】

Ｓ３０は、対象となる電子情報を読み込み、メモリやハードディスクなどの記憶媒体に記憶する。

【００３８】

この時、電子情報を暗号化した状態で記憶する場合もある。この場合は、プロテクション化した状態では元の電子情報を読み取ることは困難となり、よりセキュリティが向上する。

【００３９】

Ｓ３１は、電子情報に対して制限する操作およびその条件が定義された制限属性を、Ｓ３０で記憶した電子情報に付加する。また、必要であれば制限属性に電子情報を利用するためのアプリケーション情報を含めることもある。アプリケーション情報を含めた場合は、そのアプリケーションを使用してのみ電子情報にアクセス可能となる。

【００４０】

Ｓ３２は、電子情報へのアクセス制御を実行する制限プログラムを、Ｓ３０で記憶した電子情報に付加する。制限プログラムの内容は、対象の電子情報に対し

て指定した制限内容が制御可能であるプログラムコードが実装されていれば十分であるので、対象の電子情報や制限属性によって異なるものになっても良い。

また、制限プログラムは、電子情報を受け取る側のＯＳやプラットフォームで実行可能である必要があるため、受け取る側の利用環境に応じた実行可能な形式のプログラムコードにする。

【００４１】

Ｓ３３は、プロテクション化電子情報を出力する。プロテクション化電子情報とは、Ｓ３０で記憶した電子情報にＳ３１およびＳ３２によって制限属性および制限プログラムが付加をしたものであり、プロテクション化電子情報を利用する環境において実行可能な形式にする。

【００４２】

図４は、プロテクション化電子情報を利用する手順を示すフロー図である。プロテクション化電子情報は、利用する環境において実行可能な形式になっているが、プロテクション化電子情報を実行した際の処理は、前記制限プログラム中の前記展開処理ルーチン部にあるプログラムコードによって行われる。このフロー図は、展開処理ルーチン部の流れを説明するものである。

【００４３】

なお、制限プログラムには、展開処理ルーチン部の他に制限ルーチン部が含まれているが、制限ルーチン部はアプリケーションからのアクセスを制御するプログラムコードからなっており、その詳細については特願２０００－３５２１１３にて開示してある。

【００４４】

Ｓ４０１は、プロテクション化電子情報を起動する。起動方法は利用環境によって異なるが、例えばＯＳが実行ファイルとして起動する場合や、ＷｅｂブラウザがプラグインやＪＡＶＡアプレットとして起動する場合がある。

【００４５】

Ｓ４０２は、制限プログラム中に含まれる制限ルーチン部をコンピュータ内にロードし起動する。

【００４６】

Ｓ４０３は、プロテクション化電子情報に含まれている制限属性を取得する。制限属性に起動するアプリケーション情報が含まれている場合は、その情報を取得し起動すべきアプリケーションを特定する。制限属性に起動するアプリケーション情報が含まれていない場合は、起動すべきアプリケーションを自動判断によって特定する。

【００４７】

自動判断の方法は、例えば電子情報のタイプや拡張子からＯＳにて定義されているアプリケーションを取得する方法や、利用環境に応じてアプリケーションを特定する方法がある。

【００４８】

また制限属性に含まれている制限操作および制限条件を取得し、Ｓ４０２によって起動した制限ルーチン部に渡す。

【００４９】

Ｓ４０４は、Ｓ４０３によって特定したアプリケーションを起動する。

【００５０】

Ｓ４０５は、Ｓ４０３によるアプリケーションの起動が成功したか失敗したかを判断する。起動が成功した場合は、Ｓ４０２によって起動した制限ルーチン部が、その仕組みにより、アプリケーションのアクセスに対する監視を開始し、これ以降のアプリケーションの操作に対して制御が可能となる。

【００５１】

Ｓ４０３によるアプリケーションの起動が失敗した場合は、プロテクション化電子情報の実行を終了する（Ｓ４１４）。

【００５２】

プロテクション化の実行を終了する際に、Ｓ４０２にて起動した制限ルーチン部を終了させる場合もある（Ｓ４１５）。

【００５３】

制限ルーチン部を終了させない時は、以降のプロテクション化電子情報の起動時に、同一の制限ルーチン部を起動させる場合、その起動が速くなるという利点がある。Ｓ４１４とＳ４１５のいずれかは、利用環境に応じて選択する。

【００５４】

Ｓ４０７は、プロテクション化電子情報に含まれる元の電子情報を抜き出し、アプリケーションがアクセス可能な状態に復元する。例えば、アプリケーションがファイルの形式でアクセスするのであれば、ファイル形式に出力する。元の電子情報と同じ形式の情報に復元することで、アプリケーションからのアクセスが可能となる。

【００５５】

なお、図３のＳ３０において電子情報を暗号化している場合は、Ｓ４０７にて復号もする。

【００５６】

Ｓ４０８は、Ｓ４０７で復元した電子情報をＳ４０４で起動したアプリケーションに渡す。

【００５７】

Ｓ４０９は、アプリケーションが電子情報に対して通常のアクセスを行っている状態である。ただし、制限ルーチン部によってアクセスは制御されているため、制限属性で定義された制限の範囲でのみ電子情報が利用できる。すなわち、プロテクション化によって禁止された操作を試みた場合、制限ルーチン部によって拒否される。また、課金によって操作が許可される場合もある。

【００５８】

Ｓ４１０は、アプリケーションが電子情報を開放したことを示す。一般的にアプリケーションは、使用しなくなった電子情報を開放する。ファイル形式の電子情報の場合は、開放のことをクローズとも呼ぶ。

【００５９】

Ｓ４１１は、Ｓ４１０でアプリケーションが電子情報を開放したことをトリガーにして、Ｓ４０７にて復元した電子情報を抹消する。

【００６０】

Ｓ４１２は、アプリケーションの終了を示す。

【００６１】

Ｓ４１３は、Ｓ４１２のアプリケーション終了をトリガーにして、Ｓ４０２で

起動した制限ルーチン部を終了およびコンピュータ上から開放する。

【００６２】

Ｓ４１１およびＳ４１３は、プロテクション化電子情報を起動し、元の電子情報をアプリケーションが利用している間に必要なものの開放および抹消の処理だが、これらの処理は省略することもできる。省略した場合も、目的の電子情報に対する操作の制限は可能であるが、これらの処理を行うことで、元の電子情報の痕跡を残さないという利点がある。また、コンピュータ上のリソースを節約できるという利点もある。

【００６３】

【第２の実施形態】

図５は、ファイル形式の電子情報を提供する場合に本発明を応用した例として、第２の実施形態を示すシステム構成図である。電子情報としては、ワープロソフトで利用する文書ファイルを例にした。

【００６４】

文書ファイルを提供する側（５０）では、制限付きで提供したい文書ファイル（５０１）に対して、プロテクション化を行い（５０２）、プロテクション化文書ファイル（５０３）を作成し、このプロテクション化文書ファイル（５０３）を利用者側に提供することで、文書ファイルに対する利用者側での操作を制限する。

提供手段としては、電子メールソフトやＦＴＰソフトといったファイルを転送するためのソフトを利用して提供する方法（５１）、フロッピーディスクやＣＤ－Ｒ／ＲＷといった、記録可能かつ取り外し可能な媒体にコピーし提供する方法（５２）、ＬＡＮや公衆回線などのネットワークを用いたリモートファイルシステムを利用して提供する方法（５３）などがある。

【００６５】

いずれの方法も、プロテクション化文書ファイルはファイル形式のまま利用者側に提供される。提供されたプロテクション化文書ファイルは利用者側のコンピュータで実行可能な形式をしており、実行することで、電子情報にアクセスするためのワープロソフトが実行され、すでに述べた方法によって、ワープロソフト

で対象の電子情報が利用可能となる。しかも、利用中は制限ルーチン部によってワープロソフトのアクセスが制御されており、禁止された操作は拒否される。

【００６６】

例えば、閲覧のみ許可するために、印刷、編集または文書の転写を禁止する場合、ワープロソフトが禁止したい機能を備えたものであれば、制限ルーチン部にこれらの制御プログラムコードを含め、制限操作として印刷、編集、転写機能を指定することで実現可能となる。

また、利用時間や利用者、利用場所を限定する場合には、制限条件として、それらの条件を指定することで制限可能となる。

さらに、課金情報を制限条件に指定することで、利用者が文書ファイルを閲覧する際に、課金することも可能となる。

この例は、著作権の対象となる文書ファイルや、特定の人にのみ提供する場合に有効となる例である。

【００６７】

【第３の実施形態】

図６は、ファイル形式以外の電子情報を提供する場合に本発明を応用した例として、第３の実施形態を示すシステム構成図である。電子情報としては、画像、音楽、動画等のマルチメディア情報を例にした。

【００６８】

マルチメディア情報を提供する側（６０）では、制限付きで提供したいマルチメディア情報（６０１）に対して、プロテクション化を行い（６０２）、プロテクション化マルチメディア情報（６０３）を作成し、このプロテクション化マルチメディア情報（５０３）を利用者側に提供することで、マルチメディア情報に対する利用者側での操作を制限する。

提供手段としては、Ｗｅｂシステムを利用して提供する方法（６１）、携帯電話などの携帯端末機を用いたサービスを利用して提供する方法（６２）などがある。

【００６９】

いずれの方法も、マルチメディア情報は通信網を介して通信データとして利用

者側に提供される。提供されたプロテクション化マルチメディア情報は利用者側のコンピュータで稼動しているＷｅｂブラウザソフトや、携帯端末機のＯＳ上で実行可能な形式をしており、プロテクション化マルチメディア情報を実行することで、マルチメディア情報にアクセスするためのマルチメディアソフトが実行され、すでに述べた方法によって、対象の電子情報が利用可能となる。しかも、利用中は制限ルーチン部によってマルチメディアソフトのアクセスが制御されており、禁止された操作は拒否される。

ここで、Ｗｅｂブラウザや携帯端末機上で実行可能な形式としては、ＪＡＶＡアプレットの形式や特定のプラグインにて実行される形式などがある。すなわち、プロテクション化電子情報の形式は、利用者側のプラットフォームで実行可能な形式であり、対象のアプリケーションが起動できるものであれば良い。

なお、実行可能な形式がファイル形式であれば第２の実施形態と同じ方法にて実現される。

【００７０】

例えば、閲覧のみ許可するために、印刷、編集またはマルチメディアの転写を禁止する場合、マルチメディアソフトが禁止したい機能を備えたものであれば、制限ルーチン部にこれらの制御プログラムコードを含め、制限操作として印刷、編集、転写機能を指定することで実現可能となる。

また、利用時間や利用者、利用場所を限定する場合には、制限条件として、それらの条件を指定することで制限可能となる。

さらに、課金情報を制限条件に指定することで、利用者がマルチメディア情報を利用する際に、課金することも可能となる。

この例は、ライブ情報などをリアルタイムで提供する場合のようにファイル形式で提供が困難なマルチメディア情報や、Ｗｅｂシステムを利用した不特定多数に対する提供において課金するような場合に有効となる例である。

【００７１】

【第４の実施形態】

図７は、企業や工場などのイントラネット環境に本発明を応用した例として、第４の実施形態を示すシステム構成図である。

通信ネットワーク７０１より７０２の回線を介してルータ７０３に接続されている。７０４はWWWサーバで７０６はファイアウオールである。７０６を介して提供する電子情報が保管されているサーバ７０８に接続される。

【００７２】

７１２は７０８に接続されている企業のデータベースである。このデータベースには、顧客のリスト、営業情報、工場であれば生産、製造の技術情報、設計開発の情報等企業活動に必要な各種のデータ、情報が格納されていてクライアントである企業の社員は先に説明したような、制限の元に利用できる。職能階層に応じて利用できる情報とできない情報がある。場合によっては代表権のある役員しか開示できない情報もあって、それぞれの電子情報に制限操作や制限条件が定義されている。

【００７３】

企業内ＬＡＮ７１１を介して接続してある７１２、７１３、７１４は、企業内のクライアントＰＣ、サーバである。７１５は多機能電話機、７１６はプリンター、ＦＡＸ／コピー機である。７１７は携帯情報端末機器、ＰＤＡを７１８は携帯電話機７１９はモバイルノートＰＣを示す。これらの機器は社内、構内モバイル機器として用いる。７２０は構内移動車載端末を示す。

７１０は企業内、構内モバイル端末機器用のアンテナを示す。

【００７４】

本イントラネットは、企業だけでなく法人、研究機関、教育機関でも使用できるのをはじめ、企業外からもアクセスできる。外からの使用はセキュリテイを確保して内部の情報を利用することが可能になる。本発明によるシステムはきわめて有効である。

【００７５】

【第５の実施形態】

図８は、ホームに対して電子情報を提供する場合に本発明を応用した例として、第５の実施形態を示すシステム構成図である。ＩＴの普及によって、家庭で就労する人が増えてきた。我が国でもすでに６百万人を超えたと言われている。少子高齢化と伴にこの傾向は増加の一途にあるといえる。

【００７６】

図８において、９３の公衆回線よりホームルータ９４２に接続される。９２は公式Ｗｅｂサイトに接続している。例として、ＮＴＴドコモ社のｉモードサイトがある。９４２のルータはホームＬＡＮ９４３に接続されている。９４３は有線ＬＡＮだけではなく、ブルートース、Ｉｒｄａを使用した無線ＬＡＮでもよい。９４４はＰＣまたはホームサーバ、９４５は大画面付きの多機能電話機、９４６はＴＶ、９４７は音響ＡＶ機器、９４８はモバイル携帯情報端末機器を示す。９４１はアンテナで公衆無線網との接続を行う。９４は家、家庭を示す。

【００７７】

在宅就労は各種の企業情報、機密情報を扱うのでセキュリテイの確保は最重要課題である。公式Ｗｅｂサイト９０３から提供される電子情報は、必要に応じて利用範囲が制限されているため安全である。又、仕事だけでなく娯楽としてのコンテンツをネットワークから配信を受ける環境になってきた。９０２のＷｅｂキャストからＴＶや音楽の配信を受けて、９４６のＴＶ端末、９４７のＡＶ機器、９４８の家庭内モバイル端末で楽しんで、生活を豊かにすることができる。

【００７８】

娯楽コンテンツをネットワーク上のサイトから提供を受けた場合、料金の支払いが必要となるが、その場合は、提供する電子情報に課金条件を指定する。９０１の金融機関のサイトから自動引き落としをする際に通信する電子情報にもアプリケーションの限定や時間指定、利用者指定をすることで安全になる。この場合、なりすましを防止するために個人認証が必要になる。個人認証の方法は各種提案されているが、ＩＤ番号、電話番号のほかに機密度の高い場合は公開鍵を使用するのもよい。組織に属して家庭で就労する場合、９４４のサーバは企業から提供されたものを使用して家庭就労するという、条件を設けるのも一つのホームワーキングの方法である。

【００７９】

【第６の実施形態】

図９、公共性の高い配信サービスに本発明を応用した例として、第６の実施形態を示すシステム構成図である。

通信ネットワーク９０８は、公衆網でＩＮＮＴアーネットＩＰ、電話網ＰＳＴＮ、ＸＤＳＬ網、デジタル網ＩＳＤＮ、Ｂ－ＩＳＤＮ、ＡＴＭ、モバイル網、衛星網等を使用している。

９０４は公式のＷｅｂサイトで例えばＮＴＴドコモ社のｉモードのサイトがある。９０６はモバイル無線網のアンテナで、本実施例ではｉモードサイトに接続している。もちろんＰＨＳ、他のＰＤＣ（Ｐｅｒｓｏｎａｌ　Ｄｅｇｉｔａｌ　Ｃｅｌｌａｒ）も使用できる。特にＩＭＴ２０００は高速なので動画の伝送に優れている。

【００８０】

先に説明したように提供側の電子情報はプロテクション化されており、ユーザ、クライアントの権限や利用範囲に対して制限を設けるものである。

【００８１】

９０３はデータベースのサイトであって各種のビジネス、研究等に必要な情報が格納してある。９０２はＷｅｂキャストでデジタル放送を電子情報として提供している。９０１は金融機関のサイトで課金指定された電子情報を利用する場合、使用料の徴収をおこなう。

【００８２】

９０５はＷｅｂ上に設けられたモールで、購入の際に必要な電子情報に対してセキュリティを強化できる。特に電子情報そのものが商品である場合、その利用に対して制限することが可能となり、電子情報化された絵や映画、音楽などが安全に提供できる。購入の支払いは９０１の金融機関のサイトより行う。

【００８３】

図９の９１１は利用者のための端末機器をコンビニ、街角、広場に設置した例である。図示してないがプリンター、コピー機等も接続している。

９１３は学校、研究機関を、９１２は工場、オフィスを示す。

９１４は一般家庭での使用例で９１６は、ホームサーバを示す。近年、在宅で仕事をする人がふえてきた。通信回線の発展の恩恵によるものであって、企業内のデータ、情報を活用する場合本発明によるセキュリテイの効果が発揮する。９１５はホームルータである。

【００８４】

図９の９１９は携帯情報端末機器でモバイル機器ともいう。携帯電話機の普及は顕著で、特にｉモードの発展は急速に立ち上がった。これらの機器で利用できるサービスに本発明を利用すれば、より安全な情報の提供が可能となる。さらにＰａｌｍＯＳに見られるようにＰＤＡ（携帯情報機器）の使い勝手もよい。プリンター、インターネットカメラ、デジタルカメラを搭載または接続ができる。

【００８５】

９１８はクライアント、ユーザである。図８ではモバイラーとして９１８の人は場所を問わず、何処ででも仕事ができる。このような利用形態においても、電子情報自体にセキュリティが設定されているため、情報提供側は安心して情報を提供できる。

【００８６】

９２０は車載移動体で、モバイルインターネットによって同様に電子情報提供側からプロテクション化電子情報としてサービスを受けることができる。

【００８７】

以上の実施形態で例示したプロテクション化電子情報ついては、その一例を示しただけであって、電子情報の利用環境に合わせた実行可能な形式であれば良く、ＯＳやプラットフォームがバージョンアップなどによって変更された場合でも容易に対応でき、さらに制限プログラムの機能の範囲において、制限する操作を拡張できることは言うまでもない。

また、対象となる電子情報も、例に示したもの以外に適用可能な電子情報は多くあり、プロテクション化可能な電子情報であれば同様に制限をかけることが可能であることは言うまでもない。

【００８８】

なお、本発明におけるプロテクション化プログラムは、ＣＤ－ＲＯＭ等のディスク型ストレージ、半導体メモリ及び通信ネットワークなどの各種の媒体を通じてコンピュータにインストールまたはロードすることができる。また、プログラム製品単体として、コンピュータユーザに提供することができる。

【００８９】

さらに、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に配給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【００９０】

この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００９１】

プログラムコードを供給するための媒体としては、例えば、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ／ＲＷ、ＤＶＤ－ＲＯＭ／ＲＡＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【００９２】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）やプラットフォームなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００９３】

さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００９４】

本発明を上記媒体に適用する場合、その記憶媒体には、先に説明したフローチ

ヤートに対応するプログラムコードが格納されることになる。

【００９５】

【発明の効果】

以上の説明から明らかなように、本発明は、電子情報に制限プログラム及び制限属性を付加することでプロテクション化し、プロテクション化電子情報を利用することで電子情報への操作を制限することができる。

【００９６】

また、制限プログラムは、電子情報を受け取る側のコンピュータ上で実行可能な形式にすることにより、既存の環境にあらかじめ制限プログラム等を組み込む必要がなく、上述したような各種の不正アクセスを制限することができ、既存のアクセス権の範囲を拡張することが可能になる。

【００９７】

さらに、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができるなどの効果が得られる。

【００９８】

例えば、著作権が適用される場合など利用範囲を制限したい電子情報を提供するにあたって、プロテクション化した電子情報を提供することにより、受け取った側での利用範囲を制限できるといった効果が得られる。

【図面の簡単な説明】

【図１】

本発明の実施形態を示すハードウェア構成図である。

【図２】

本発明に係るプロテクション化電子情報の構成を示す図である。

【図３】

本発明におけるプロテクション化の手順を示すフロー図である。

【図４】

本発明におけるプロテクション化電子情報に対して元の電子情報にアクセスする手順を示すフロー図である。

【図５】

電子情報の例として文書ファイルの提供に本発明を応用した第２の実施形態を示す図である。

【図６】

電子情報の例としてマルチメディア情報の提供に本発明を応用した第３の実施形態を示す図である。

【図７】

企業内のイントラネットに本発明を応用した第４の実施形態を示すシステム構成図である。

【図８】

ホームに本発明を応用した第５の実施形態を示すシステム構成図である。

【図９】

公共性の高い配信ネットワークに本発明を応用した第６の実施形態を示すシステム構成図である。

【符号の説明】

１０　電子情報を提供する側の情報処理装置

１１　電子情報を受け取る側の情報処理装置

１２　通信ネットワーク

１００、１１０　コンピュータ

１０１　電子情報

１０２、１１３　取り外し可能ディスクドライブ

１０３、１１２　ハードディスクドライブ

１１１　プロテクション化電子情報

１１４　キーボード、マウスなどの入力装置

１１５　プリンタ、ＦＡＸ、コピー機などの出力装置

１１６　ディスプレイなどの表示装置

２０　プロテクション化電子情報

２１　制限プログラム

２２　制限属性情報

２３　元電子情報

２１０　展開ルーチン部

２１１　制限ルーチン部

２２０　対象アプリケーション

２２１１　制限操作１

２２１Ｎ　制限操作Ｎ

２２２１　制限条件１

２２２Ｎ　制限条件Ｎ

５０、６０、８０、９０　電子情報提供側

５０１　一般的な文書ファイル

５０２、６０２　プロテクション化の処理

５０３　プロテクション化文書ファイル

５１　メールやＦＴＰ等による情報提供方法

５２　ＦＤ等の記憶媒体を利用した情報提供方法

５３　ネットワークにて共有

５４、６３、８５、９０９　電子情報利用者側

６０１　画像、音楽、動画等のマルチメディア情報ファイル

６０２　プロテクション化

６０３　プロテクション化したマルチメディア情報

６１　Ｗｅｂページにて公開

６２　携帯用端末へのサービス

７０１　通信ネットワーク

７０２　通信ライン

７０３　ルータ

７０４　Ｗｅｂサーバ

７０５　接続線

７０６　ファイアウォール

７０７　接続線

７０８　電子情報提供サーバ

７０９　携帯電話端末

７１０　構内無線アンテナ

７１１　ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）

７１２　情報格納ファイル

７１３、７１４，７１５　ＰＣ、サーバ

７１６　多機能電話機

７１７　ＦＡＸ、プリンター、コピーなどの出力装置

７１８　携帯情報端末機器

７１９　携帯電話端末

７２０　ノートＰＣ

７２１　構内移動車載端末機器

８０１　銀行、金融機関

８０２　Ｗｅｂキャスト

８０３　Ｗｅｂサイト

８０５　無線基地局

８２　通信ネットワーク

８３　通信ライン

８４　家庭、在宅就業

８４１　ホーム無線アンテナ

８４２　ホームルータ

８４３　家庭内ＬＡＮ

８４４　ホームサーバ

８４５　多機能電話機

８４６　ＴＶ

８４７　音響機器

８４８　携帯情報端末機器、携帯電話機、ＰＤＡ

９０１　銀行、金融機関

９０２　Ｗｅｂキャスト

９０３　データベース

９０４　Ｗｅｂサイト

９０５　Ｗｅｂモール

９０８　通信ネットワーク

９１０　通信ライン

９１１　コンビニ、街角ターミナル

９１２　企業、工場、オフィス

９１３　学校、研究機関

９１４　家庭、在宅就業

９１５　ホームルータ

９１６　ホームサーバ

９１７　無線基地局

９１８　ユーザ、クライアント

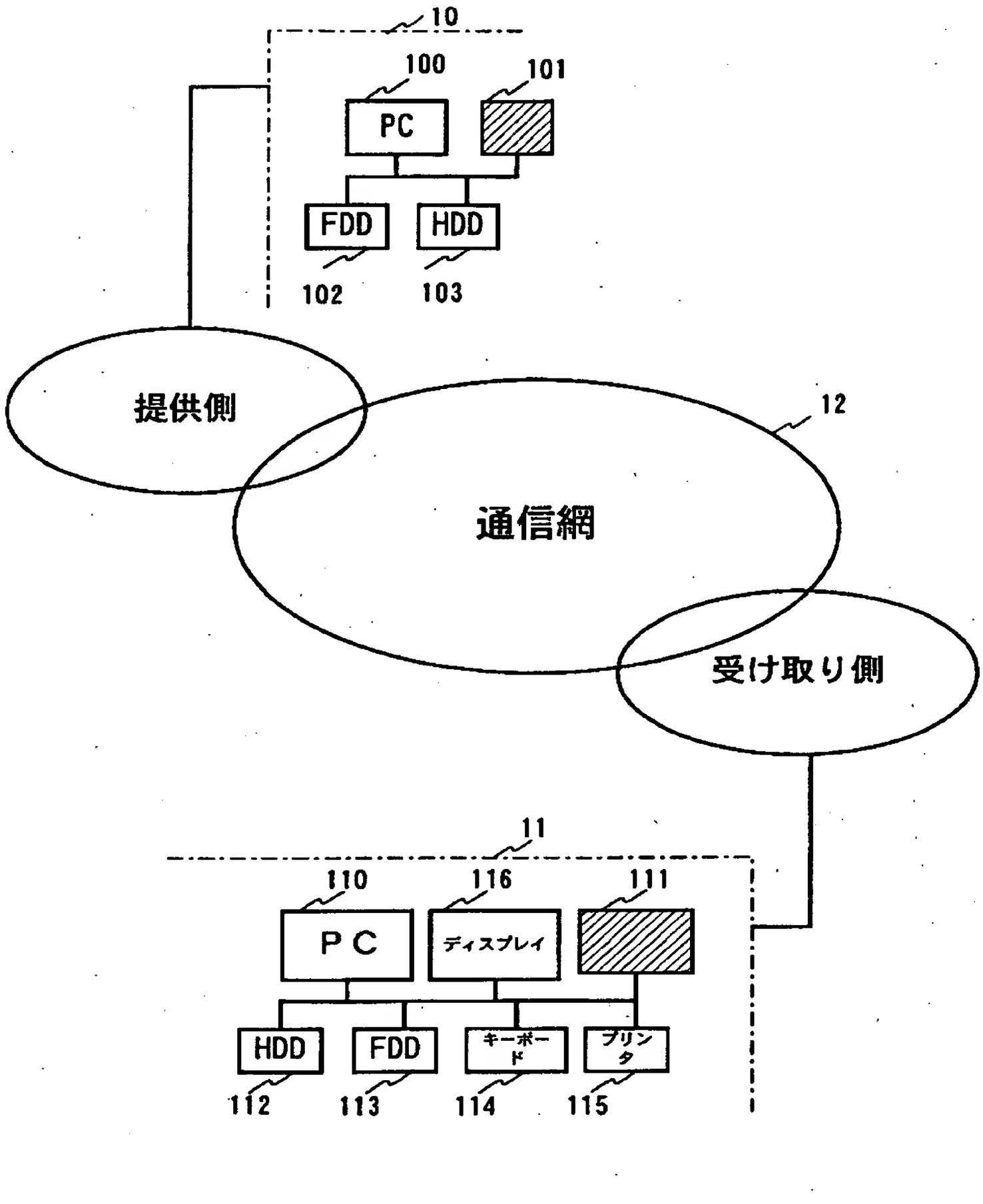
９１９　携帯情報端末機器、携帯電話機、ＰＤＡ

９２０　車載移動端末機器

９２１　携帯電話端末

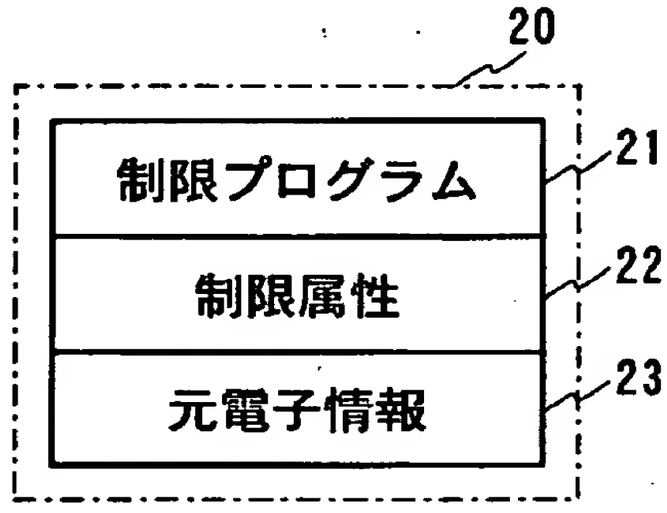
【書類名】　　図面

【図１】

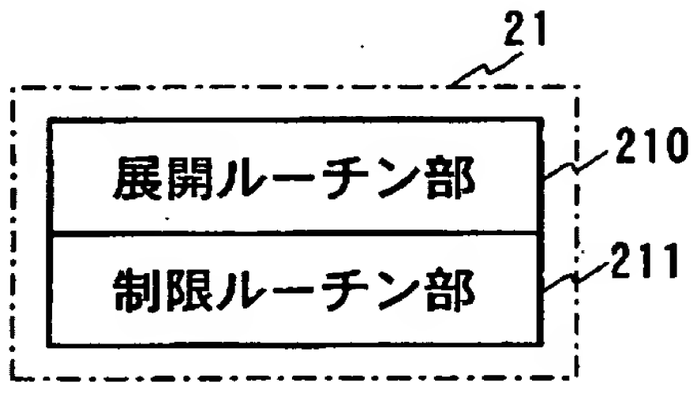

10
100
101
PC
FDD
HDD
102
103
提供側
12
通信網
受け取り側
11
110
116
111
ＰＣ
ディスプレイ
HDD
FDD
キーボード
プリンタ
112
113
114
115

【図２】

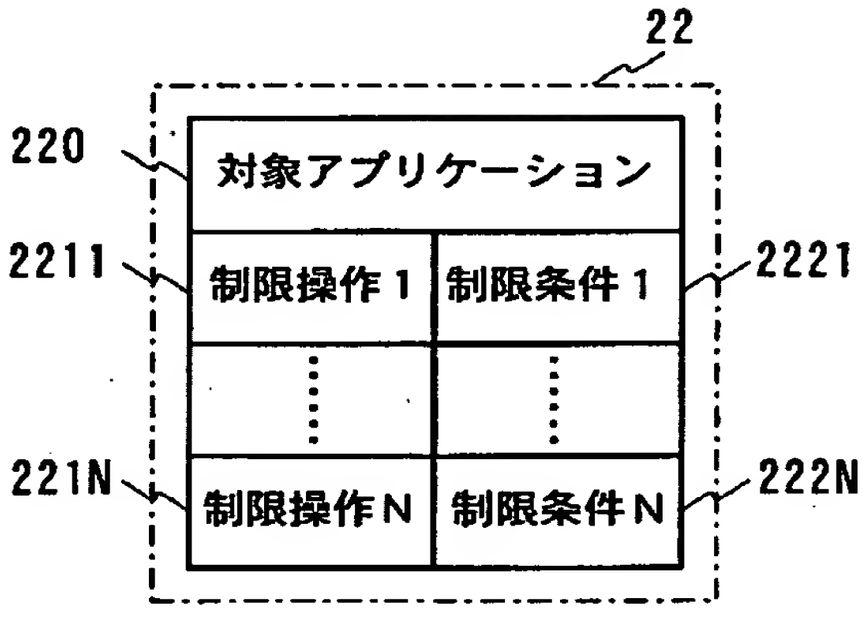
（ａ）プロテクション化電子情報



（ｂ）制限プログラム

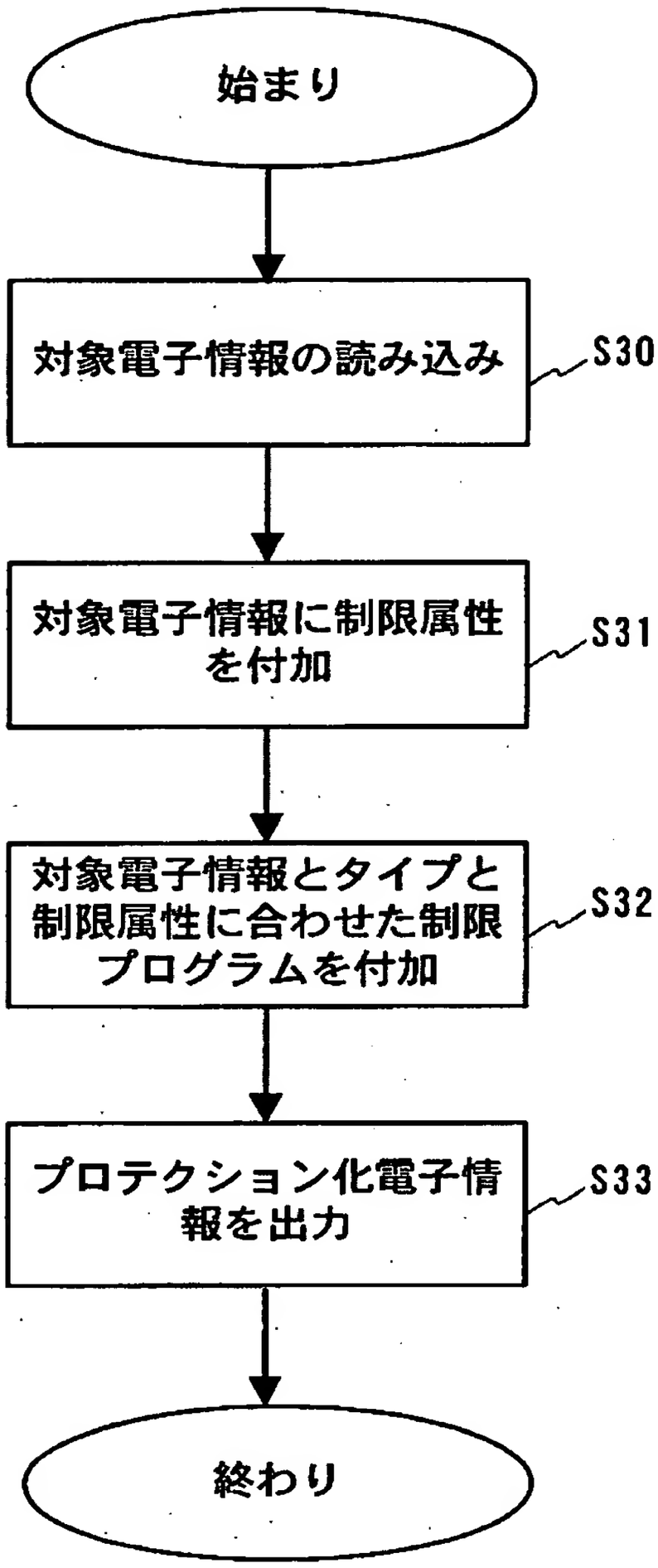


（ｃ）制限属性

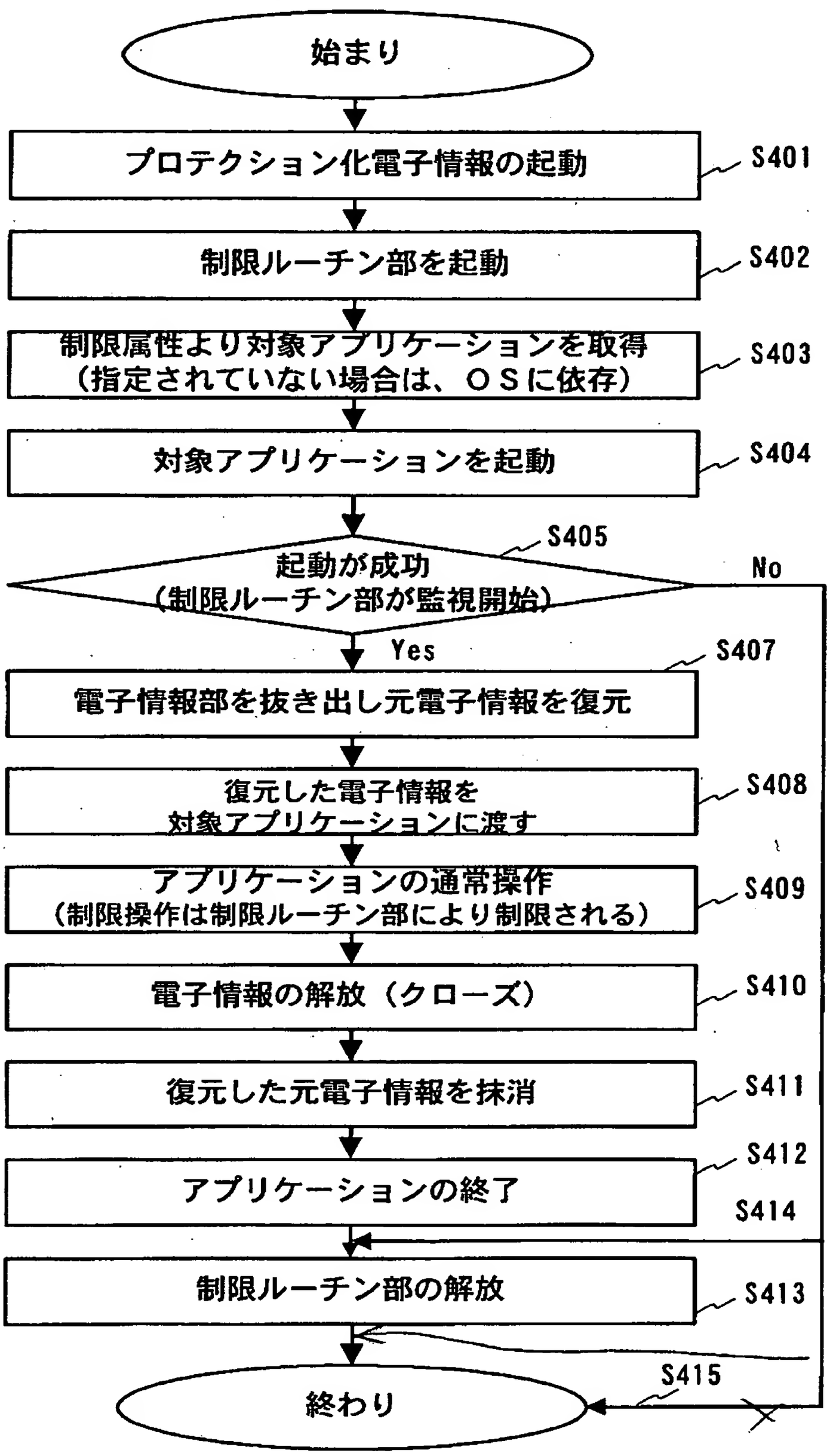


【図３】

プロテクション化の手順

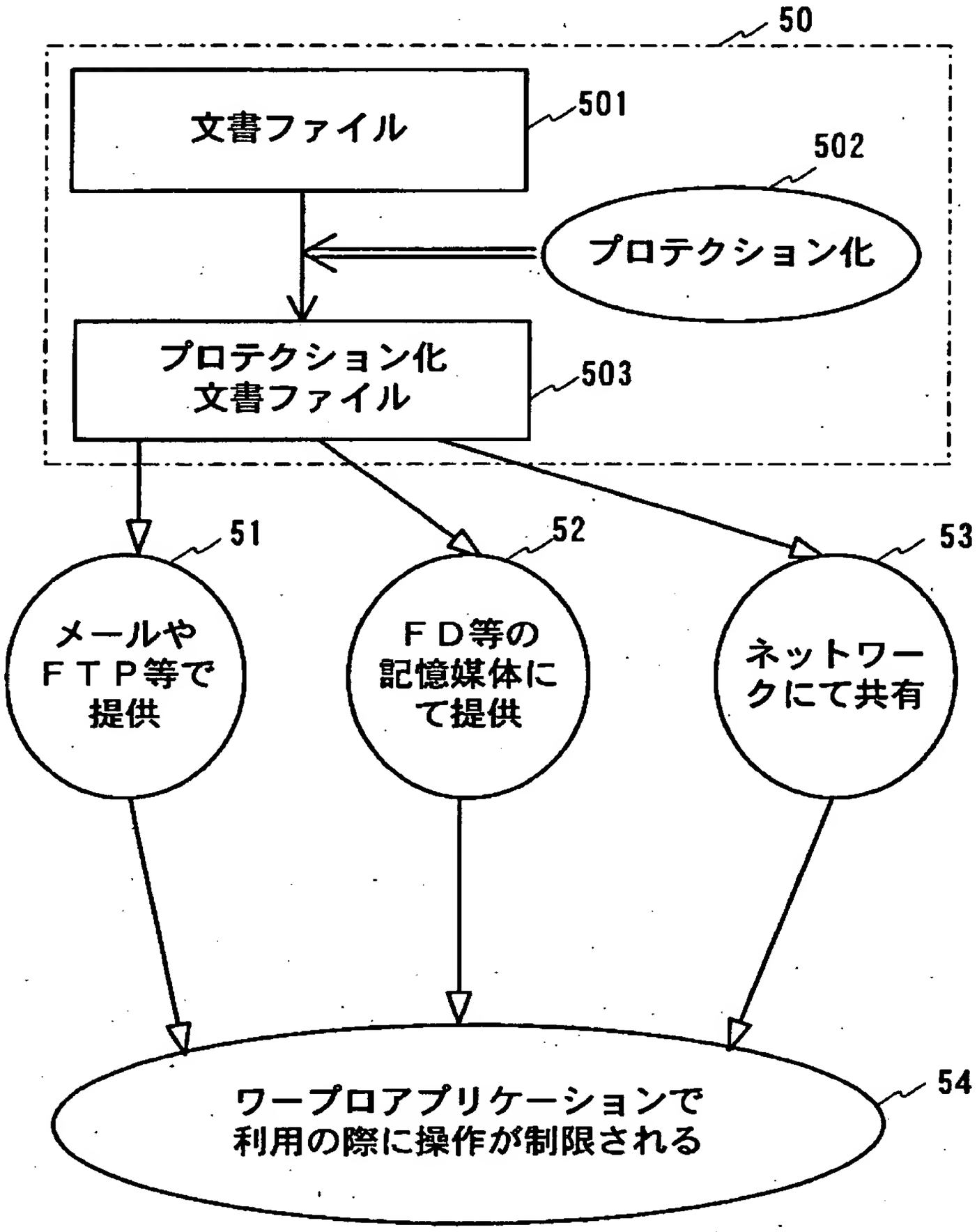


【図４】


展開ルーチン部の処理フロー
始まり
プロテクション化電子情報の起動
S401
制限ルーチン部を起動
S402
制限属性より対象アプリケーションを取得
（指定されていない場合は、ＯＳに依存）
S403
対象アプリケーションを起動
S404
S405
起動が成功
（制限ルーチン部が監視開始）
No
Yes
S407
電子情報部を抜き出し元電子情報を復元
復元した電子情報を
対象アプリケーションに渡す
S408
アプリケーションの通常操作
（制限操作は制限ルーチン部により制限される）
S409
電子情報の解放（クローズ）
S410
復元した元電子情報を抹消
S411
アプリケーションの終了
S412
S414
制限ルーチン部の解放
S413
終わり
S415

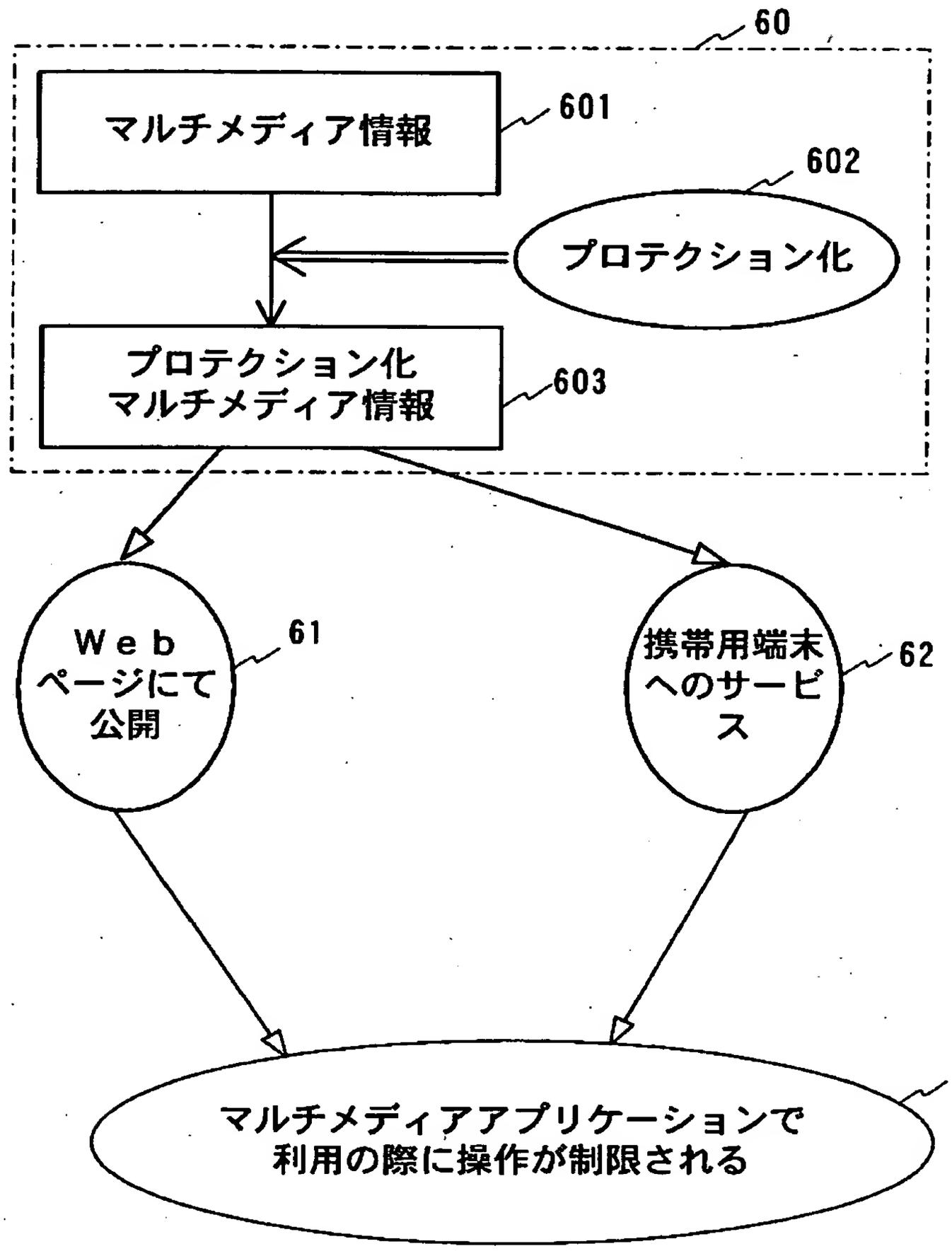
【図５】

文書ファイルをプロテクション化する例

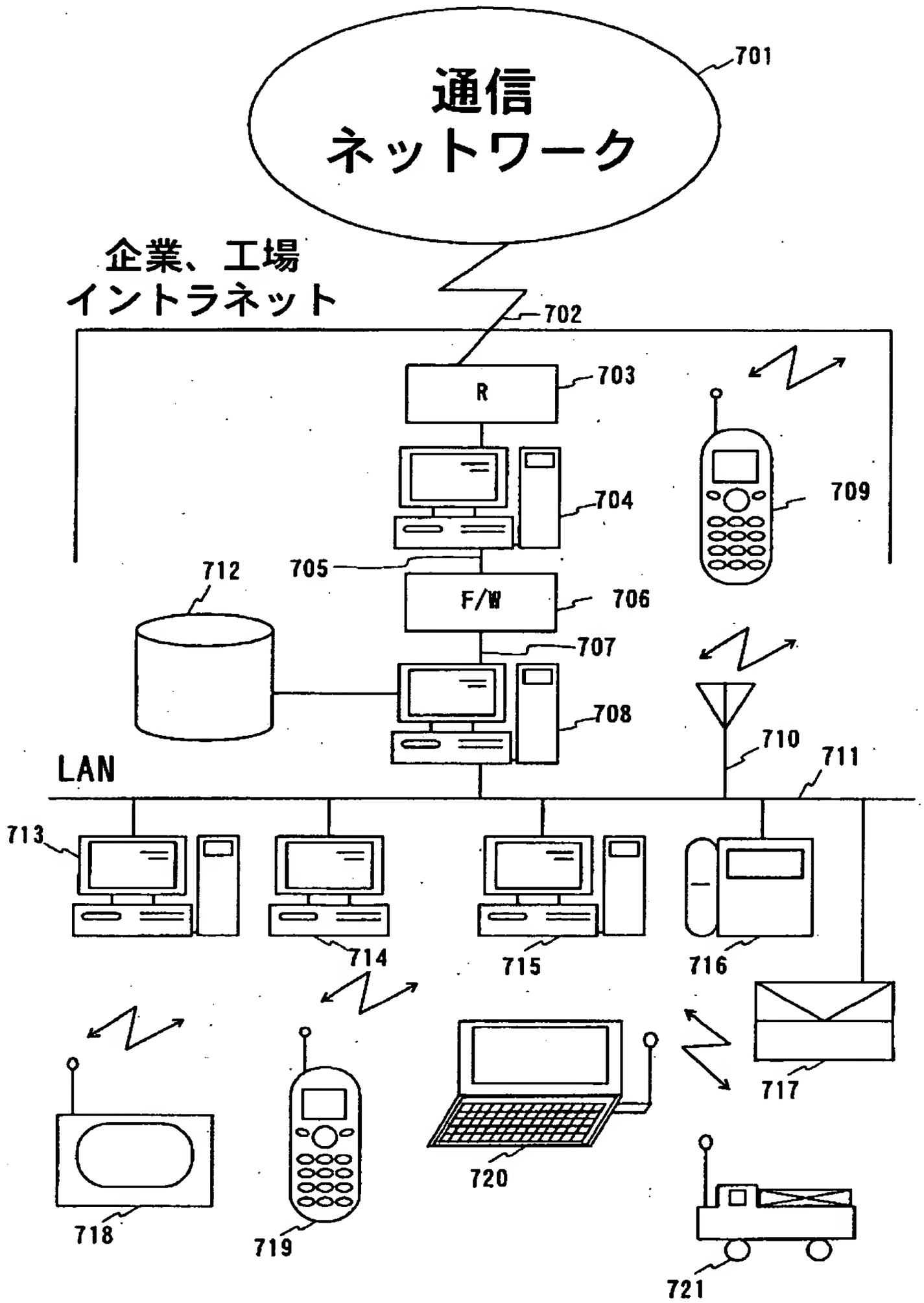


【図６】

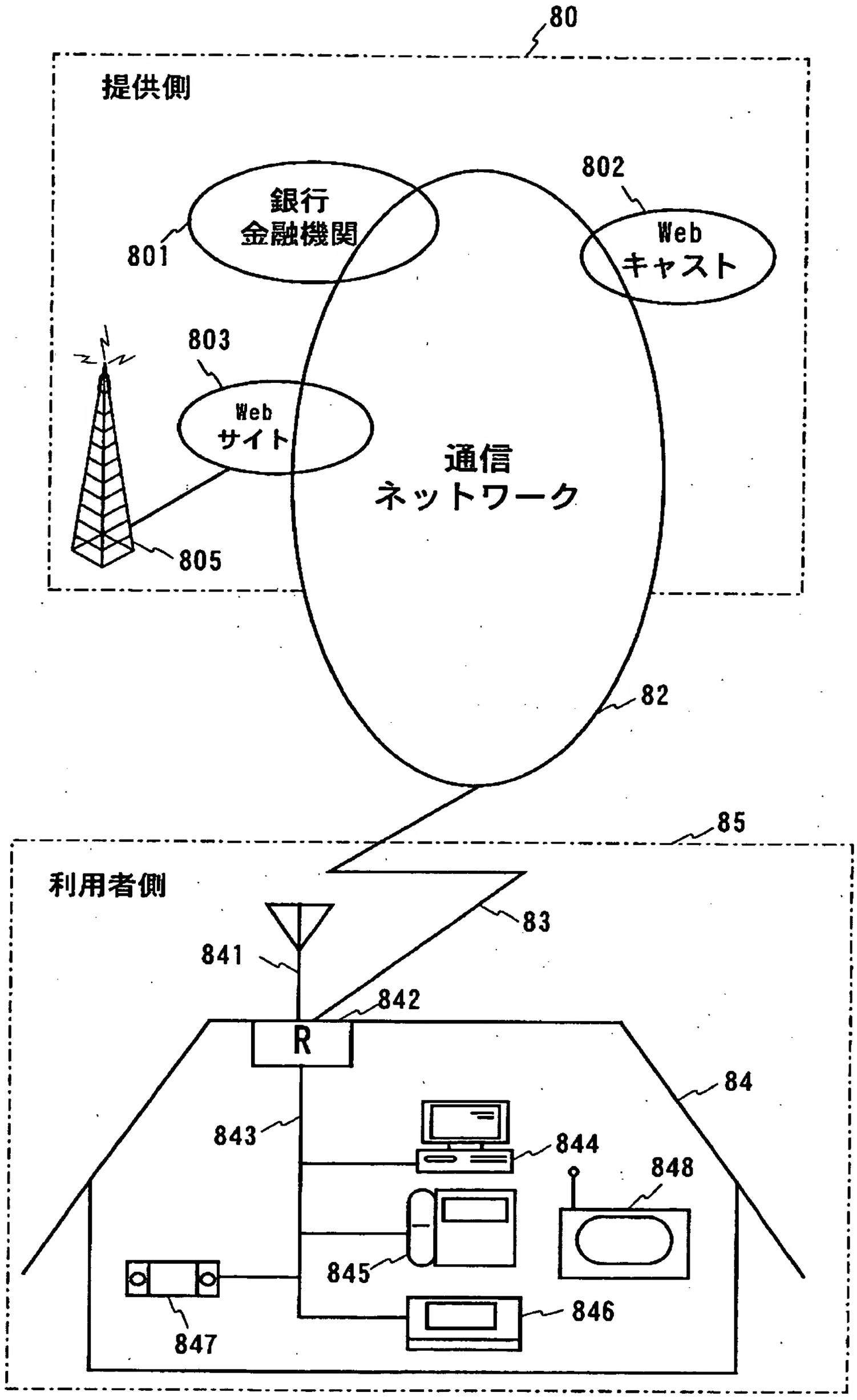
マルチメディア情報をプロテクション化する例
（画像、音楽、動画等のファイル）



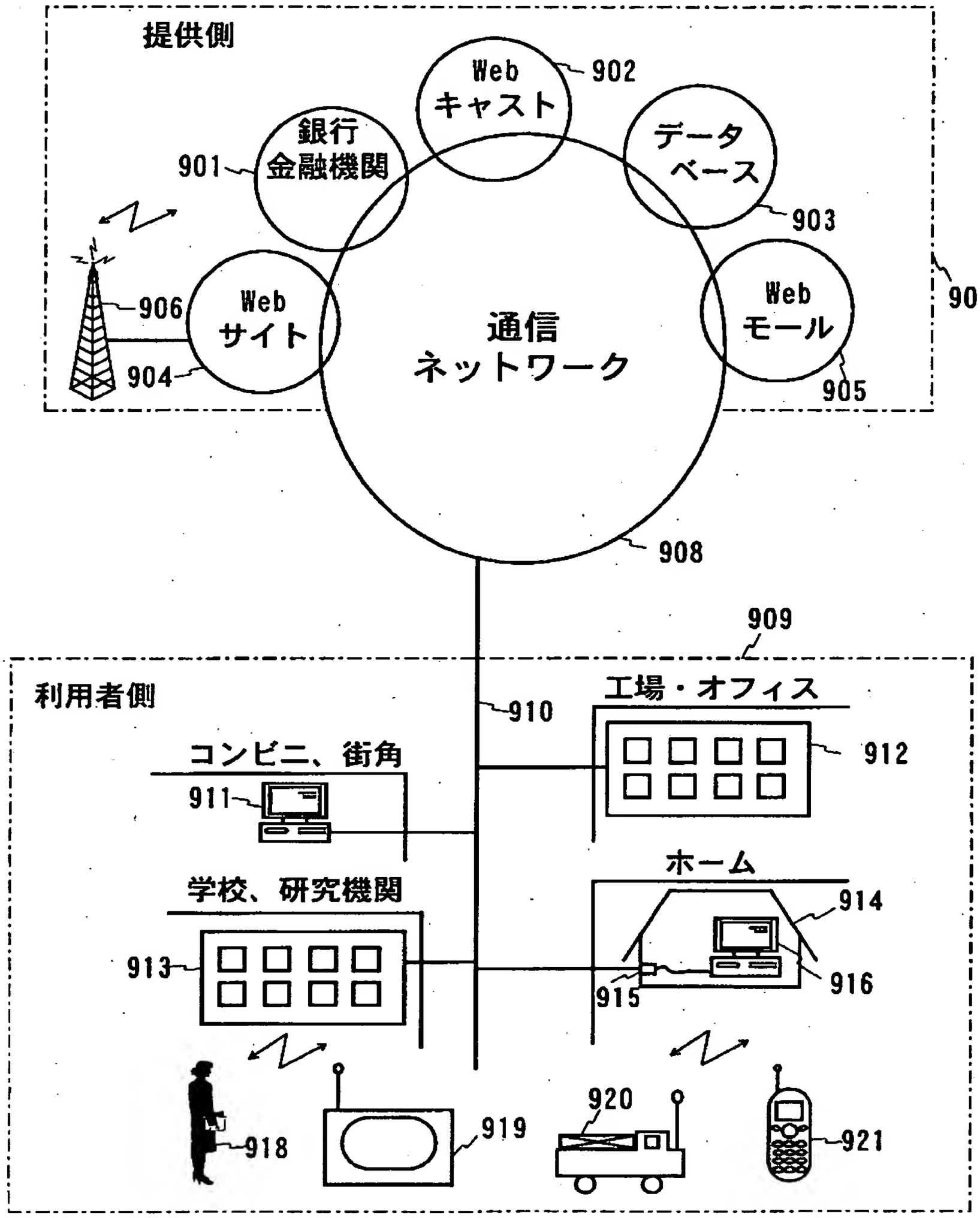
【図７】


通信
ネットワーク
701
企業、工場
イントラネット
702
R
703
704
705
F/W
706
707
708
709
710
711
712
LAN
713
714
715
716
717
718
719
720
721

【図８】


80
提供側
801
銀行
金融機関
802
Web
キャスト
803
Web
サイト
通信
ネットワーク
805
82
85
利用者側
83
841
842
R
84
843
844
848
845
846
847

【図９】


提供側
Web
キャスト
902
銀行
金融機関
901
データ
ベース
903
90
Web
モール
905
Web
サイト
906
904
通信
ネットワーク
908
909
利用者側
910
工場・オフィス
912
コンビニ、街角
911
ホーム
914
学校、研究機関
913
915
916
918
919
920
921

【書類名】　　要約書

【要約】

【課題】　電子情報に対する操作の禁止または制限を拡張し、拡張した禁止または制限操作を実現するプログラムを事前にコンピュータに導入することなく、またＯＳやプロセスを変更することなく、電子情報に対する操作を制御すること。

【解決手段】　制限内容に応じた制限プログラムと制限情報を電子情報に付加し、電子情報の利用時にこの制限プログラムを実行し、アクセスの可否を制御する。この制限プログラムは、電子情報にアクセスするアプリケーションまたはオペレーティングシステムからの操作要求を電子情報にアクセスする前に捕捉し、その捕捉した操作要求と制限情報によってアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡しその結果を要求アプリケーションに返し、アクセス権限がなければ当該操作要求を拒否するか、制限情報に応じて課金することで許可する。この制限プログラムの詳細は特願２０００－３５２１１３にて開示してある。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔５０００８３２２６〕

１．変更年月日　　２０００年　２月２５日
　［変更理由］　新規登録
　　住　所　　東京都中央区月島１丁目２番１３号
　　氏　名　　ハミングヘッズ株式会社